Crime Mapping and Data Confidentiality Roundtable July 8-9, 1999

Sponsored by: National Institute of Justice, Crime Mapping Research Center

What Security Measures are Available for Data Sharing over Internet or Intranet Environments, and How Can They be Shared with Local Agencies?

by
Robert Cheetham
Senior GIS Developer, City of Philadelphia
Mayor's Office of Information Systems

While the Internet has enjoyed explosive growth over the past decade and is now being credited with driving the U.S. economy, 'trust' is one concept not yet associated with it. Viruses spread through e-mail, hacks resulting in the defacing of corporate and public agency sites, stolen passwords, credit card fraud and a host of other ills, have become synonymous with the Internet. But trust is precisely the issue preventing more widespread use of public computer networks for a variety of appropriate purposes. The conventional means of ensuring trust are not applicable in this new environment. Despite this dearth of means for ensuring trust, the presence and ease with which Internet-based technologies can now be deployed has tempted local agencies to increasingly explore the possibilities inherent in wide-spread network connectivity. There is clearly a need for attention to the security issues related to these environments and to provide the tools to address the needs of local law enforcement and public safety agencies.

The question of security on IP-based networks, however, is not straightforward. There is a bewildering array of possible situations, each of which brings its own very different issues, opportunities, risks and responses. First, some terminology. In the beginning, there were private networks. The Ethernet LANs that connect the computers inside each of our offices are private networks. When these private networks are extended to another site or building, they are commonly referred to as WANs, or Wide Area Networks. A university campus, a large municipal government or corporate campus frequently operate as a WAN. When these Local and Wide Area Networks are operated using the Internet-based TCP/IP protocols, they are often referred to as intranets. Increasingly, corporations, large cities and state/federal governments are using the commonly available and increasingly inexpensive hardware and software previously associated with the Internet to make available information and

analytical applications to their employees through web browsers and e-mail clients. At this point, these are still private networks, with no possibility of invasion from the Internet or hackers. The security issues are entirely internal, though not insignificant.

However, inevitably, these employees will come to desire connectivity to the outside world. Initially, this might be provided by an e-mail router that allows mail out but filters incoming mail. While the Internet was popularized through e-mail, organization quickly extend their connectivity to the Internet by allowing access via FTP and HTTP (Web). Browsing the web from inside a private network, requires additional security measures to protect the data and resources on the network. This is usually accomplished through the use of a firewall and proxy server. These devices serve to open a single, well-defined, monitored passage to the outside world and restrict the kinds of data and messages that are allowed flow in and out. Some organizations may find it necessary to erect multiple firewalls and employ full-time security professionals to monitor for security threats even these limited windows on the outside world.

Eventually, the organization often decides it would also like to give some limited access to its data and network by its friends and allies or by its own mobile/roaming employees. Since this means allowing outsiders to enter the private network, additional security measures become necessary, including encryption and advanced authentication procedures. These extended networks that allow access from the outside are usually called extranets.

Having established some terminology, we might now turn to means of securing transactions across these various environments such as policy brokers, password authentication, firewalls, digital certificates, VPNs, encryption, data generalization and substitution, aggregation, field suppression, etc. But these tactics can only be deployed effectively within a context, and it may be most helpful to consider, instead, several scenarios in which these four environments might be deployed to serve the data sharing needs of local public safety organizations. There are several typical situations that might be imagined given the technology currently available.

Scenario 1: Intranet – Local Agency HQ wants to enable district/precinct offices to access crime data and visualization applications hosted on a web servers at the HQ by using web browsers and FTP clients over the City's WAN.
Assuming that the City's WAN is a private network or, at least, behind a firewall monitored by security personnel, access by malicious outsiders is not the concern. Rather, access by other City agencies needs to be prevented. This can be prevented through the use of passwords, though password maintenance can be an administrative headache for a large agency. Even without passwords, all web and FTP servers currently on the market allow IP address filtering. In order to participate in the intranet, each computer must be assigned an IP address. Assuming these IP addresses are known, access to all data and applications can easily be limited to this approved list. It is often desirable to maintain a log of data requests and transmissions as well. If an additional layer of security is desired, sensitive data can be transmitted using a

secure form of HTTP called Secure Sockets Layer (SSL). This is the de facto standard for transmission of credit card numbers over the internet and while it is slower, all data passing between the web browser and server are encrypted.

If the agency also wants to allow open file browsing across the entire network, it usually becomes necessary to establish centralized directory services in which file access policy is tied to a password and identity. This directory-based approach is a still maturing marketplace, however, and administrative requirements are significant. In any case, this is often not an appropriate solution for crime data sharing as the officers and detectives need simple and powerful query, analysis and visualization tools of integrated data sets rather than access permissions to a particular file stored at a particular location provided by the directory services.

Scenario 2: Internet Maps – Local Agency wants to make crime maps and data available to the public over the Internet.
The security concerns in this scenario are virtually non-existent. There are no issues surrounding authentication or encrypted transmission. Rather, the real questions are policy and privacy decisions. How much data is made available and in what format? There are several approaches being deployed on an experimental basis across the country. Many agencies choose some form of masking. Data elements that allow identification of individual victims of violent crime are often not made available. Generalization and aggregation are also effective tactics. Aggregation involves summing the crime totals by a reporting unit such as beat, sector or neighborhood. Generalization refers to abstracting the point locations somewhat by moving the points to intersections, rounding off the address numbers, or even displaying raster-based density surfaces rather than points. Some agencies make available detailed maps of crime locations, but they are not 'live' maps that allow identification of the details of each crime by clicking on the location.

Scenario 3: E-mail – Local Agency A wants to regularly exchange data with Local Agency B without having to hand deliver it.
The scenario is essentially what we all do when we send each other e-mail attachments. The fact remains, however, that e-mail, including attachments, is easily intercepted and read by others. Assuming that the data being exchanged is sensitive, the best approach will be to encrypt the e-mail before sending it. This can be accomplished using a technology called Pretty Good Privacy. PGP is available for free download and installation on most personal computers and integrates well with most common e-mail programs. The only difficulty is that the person at the receiving end must be able to decrypt the messages. The encryption technology behind PGP is the same as that incorporated in products sold to corporations for the same purpose and several commercial versions are also available, most notably from Network Associates, Inc.

Scenario 4: Protected Internet – Local Agency wants to make crime maps and data

available only to neighborhood watch groups and other community organizations rather than to the general public. There is a desire to share the data but not the resources to enable access by the entire community.
Again, masking of sensitive data and generalization of point locations may be necessary. Passwords can be used to restrict access to some extent and if there is simply a question restricting the number of people accessing the data to the infrastructure available, this may be sufficient. There is growing support for a strong encryption standard for the transmission of passwords called Message Digest Authentication. It is an extension to the web's HTTP protocol and will be widely available in Microsoft products with Windows 2000. It is already supported by Apache web servers and Internet Explorer 5.0. Since only the password is encrypted, the work of encrypting and decrypting all of the data transfers is significantly less. Under other circumstances, however, it may be necessary to provide the ability to access the internal network through the use of an extranet.

Scenario 5: Extranet – The Local Agency wants to allow secure access to its internal data and applications by neighboring and federal/state agencies – or – a regional crime analysis and mapping center needs to allow local agencies to deposit regular data updates in a secure fashion.
This scenario is the most challenging, but the technology to make it possible is increasingly being commoditized as corporations attempt to build their own secure networks with suppliers and partners. The approach in this case has historically been to either provide dial-up access to an internal modem bank or to lease a dedicated line, both expensive and high maintenance solutions. The latest set of technologies that make this possible, however, are called Virtual Private Networks (VPN). VPNs allow the outside agency to use an existing Internet Service Provider (ISP) to carry encrypted traffic through a virtual tunnel in and out of an organization's private network. A special router, called a VPN switch, usually handles the job of encryption and authentication at the back end. A VPN client at the external site does the job of decryption. VPNs are still quite complex to deploy and while three standards (PPTP, IPSec and L2TP) have emerged in the last year as dominant, support for them varies. The switches start at under $10,000 for a few dozen users and go to $50,000+ for 5,000 or more users. Recently, Bell Atlantic and UUNet have announced 'managed VPN' services that will allow an agency to outsource the equipment and maintenance costs. This will undoubtedly be the best solution for most agencies as the lack of skilled personnel will otherwise make the prospect of VPN deployment daunting, at best.

Each of the above solutions arrives with its own training, policy, cost, reliability, administration and maintenance concerns. Each approach must weigh the resources available against the state of the technology and local agencies must be willing to accept the possibility that it may be best to wait a few years for the technology to mature. The acceleration of this maturation process will be aided by several measures: 1) legitimization of digital certification as legally binding – measures to this affect have

been passed or are being considered by most states; 2) widespread availability of strong encryption technologies; 3) encouragement of internet-based commerce – much of the rapid development of security technologies and standards for the Internet is being driven by commercial activity – the faster the corporate world can deploy easy-to-use, secure technologies, the faster these methods will become available at a reasonable cost and within the framework of an accepted set of standards; 4) primary consideration of security concerns in all transfers of sensitive data, whether or not this occurs over IP-based networks; 5) cultivation of personnel trained in the technologies available and how to deploy them; 6) where possible, regional integration of data sharing infrastructure in order to provide a single point of access as well as a shared pool of trained personnel; 7) national guidelines for making available to the public visualizations of crime data.

University of Pennsylvania